# EXHIBIT 3

# Acceptable Use Policy

| | |
|---|---|
| **Identifier** | P.IT.001 |
| **Effective Date** | March 1, 2022 |
| **Applicable to** | All employees, contractors, external parties with access to the Bill.com network |
| **Policy Owner** | VP, Information Technology |
| **Review Cycle** | Annual |

## 1. Acceptable Use Overview

Acceptable use defines how individuals must handle organizational resources including actions that are allowed and not allowed.

## 2. Purpose

The intent of the Acceptable Use Policy is to communicate expectations for Bill.com employees and contractors regarding access to and use of Bill.com information assets which include but not limited to information, electronic and computing devices, and network resources to conduct Bill.com business or interact with internal networks and business systems, whether owned or leased by Bill.com, the employee, or a third party. These rules are in place to protect users and Bill.com. Inappropriate use exposes Bill.com to risks including virus attacks, compromise of network systems and services, and legal issues.

## 3. Scope

The Bill.com Acceptable Use Policy applies to all employees, contractors, third parties, and any other individual or entity for which we employ, conduct business with and/or obtain services that require access to our network or sharing of data.

This policy is to be enforced in all jurisdictions where Bill.com and its subsidiaries operate in accordance with local or regional laws and regulations.

# 4. Policy

## 4.1 General Use and Ownership

- Bill.com confidential information stored on electronic and computing devices whether owned or leased by Bill.com, the employee or a third party, remains the sole property of Bill.com
- Users shall bear the responsibility for knowing and complying with applicable state and federal laws, rules and regulations, and contractual obligations when accessing Bill.com information assets
- Bill.com provides information assets as a resource to all employees, contractors, consultants, temporary and other workers. Each individual shall be responsible for properly using and protecting those resources
- Users have a responsibility to promptly report the theft, loss or unauthorized disclosure of Bill.com proprietary information
- Users may access, use or share Bill.com proprietary information only to the extent it is authorized and necessary to fulfill their assigned job duties
- Use of external information systems to access the Bill.com system is prohibited unless the appropriate security controls are verified and deemed adequate with an approved connection or processing agreement by InfoSec and Legal
- Users' access to Bill.com information assets (e.g., customer data) shall be restricted to need-to-know and minimum necessary
- Users shall be responsible for the use and protection of Bill.com information resources by using effective access controls (e.g., passwords) and by safeguarding those access controls (e.g. disclosing passwords)
- Users are required to handle, label, and store confidential data in accordance with the Data and Information Classification Policy
- Connection to the Internet, or use of a website, is a privilege and not a right. Any abuse of that privilege can result in legal and/or administrative action
- Users shall be allowed to use Bill.com information assets:
    - To which they have been granted authorized access
    - For Bill.com business and research purposes
    - For incidental personal use (Employees are responsible for exercising good judgment regarding the reasonableness of personal use.)
- Users shall be allowed incidental personal use so long as those activities are legal and do not violate:
    - Bill.com policies, including our Code of Conduct and Ethics
    - Contractual obligations
    - The safety, security, privacy, reputational and intellectual property rights of others.
    - Applicable restrictions on political or commercial activities
- Users are prohibited from syncing their personal iCloud and/or gmail/g-drive accounts on their corporate-issued devices
- The IT team provides appropriate hardware and software to employees for Bill.com business use only

- Bill.com reserves the right to audit and monitor networks and systems activities on a periodic basis to ensure compliance with this policy. In the event that use is determined to be contrary to Bill.com policy or applicable law, appropriate measures shall be taken
- Users shall ensure that unattended equipment has appropriate protection
- Users shall log-off computing devices when the session is finished (i.e., not just switch off the PC screen or terminal)
- Users shall safeguard unattended information system output devices (e.g., printers) to prevent unauthorized individuals from obtaining the output

*Note: *Unless otherwise approved, employees and contractors with access to sensitive production data (i.e. bank partner data) seeking to temporarily work outside of U.S. or other approved jurisdiction or country of employment will have all such access disabled until return to primary location to ensure data is not processed outside of authorized boundaries*

## 4.2 Acceptable Password Use

- Passwords must be kept confidential and must not be written down or recorded electronically
- Passwords and accounts must not be shared. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited
- Personal and Bill.com (business) passwords must be different
- Temporary passwords shall be changed at the first log-on.
- Passwords must meet the minimum requirements of Bill.com's Password Policy
- All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 5 minutes or less

## 4.3 User Acknowledgement and Agreement

User will not engage in the following activities:

- Disclose or share any Bill.com confidential data to unauthorized parties without proper authorization or approval
- Post, use or transmit content that they do not have the right to post or use, for example, under intellectual property, confidentiality, privacy or other applicable laws
- Post, use or transmit unsolicited or unauthorized content, including, but not limited to, advertising or promotional materials, "Junk mail", "Spam", "Chain letters", "Pyramid schemes", political campaign promotional material, and any other form of unsolicited or unwelcome solicitation or advertising
- Infringe upon copyrighted material of any kind, including the unauthorized downloading, copying, displaying, and/or distributing of copyrighted material. All such works should be considered protected by copyright law unless specifically stated otherwise. Any use of Bill.com information assets (e.g. network, email system, website, etc.) to access, display, send, transfer, modify, store or distribute copyrighted material (e.g., video/movies, music/audio, images, documents, software, text, etc.) is strictly prohibited
- Post, use or transmit content that contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer

software or hardware or telecommunications equipment or otherwise interfere with or disrupt Bill.com information assets
- Post or transmit content that is harmful, offensive, obscene, abusive, invasive of privacy, defamatory, hateful or otherwise discriminatory, false and misleading, incites an illegal act, or is otherwise in breach of one's obligations to any person or contrary to any applicable laws and regulations
- Intimidate or harass another
- Use or attempt to use another employee, contractor, consultant, temporary, and other workers' account, service, or personal information
- Remove, circumvent, disable, damage or otherwise interfere with any security related features
- Attempt to gain unauthorized access to Bill.com information assets, other user's accounts, computing devices or networks connected to Bill.com information technology resources, through hacking, password mining or any other means, or interfere or attempt to interfere with the proper working of Bill.com information assets or any activities conducted through those information assets
- Impersonate another person or entity, or falsely state or otherwise misrepresent one's affiliation with a person or entity
- Conduct any activities with the intention of creating and/or distributing malicious programs using Bill.com's network (e.g., viruses, worms, Trojan Horses, etc.)
- Install or use unauthorized or malicious software, or obtain data and software from external networks
- Fail to exercise appropriate caution when opening emails, attachments or accessing external web sites

All users shall read and acknowledge the Acceptable Use Policy before receiving access to information assets, be responsible for appropriately securing their computers and other electronic devices from misuse or theft by others; and for avoiding any use that interferes with others' legitimate access to and use of Bill.com information assets.

### 4.4 Monitoring

- While Bill.com desires to maintain privacy and to avoid the unnecessary interruption of activities, Bill.com reserves the right to investigate unauthorized or improper use of computing devices, which may include the inspection of personal data stored or transmitted on Bill.com's network. In the event that use is determined to be contrary to Bill.com policy or applicable law, appropriate measures shall be taken
- Information asset owners shall approve the use of information assets and take appropriate action when unauthorized activity occurs

## 5. Roles and Responsibilities

| Role | Responsibilities |
|---|---|
| IT Team | Enforce the IT policy |

| | |
|---|---|
| Infosec | Support the development and enforcement of policies and standards |

## 6. Policy Governance

This policy is owned by the individual designated as the VP, Information Technology of Bill.com.

Review of this policy is required at a minimum annually in line with the last review date indicated in the Revision History section of this document or at the time of significant changes to the internal or external environment.

All new employees and contractors must complete mandatory security awareness training inclusive of review of this policy and supporting security policies.

Policy exceptions must be submitted via request to InfoSec Governance Risk and Compliance (GRC) for review and decisioning. If approved, an exception is effective for one year from the approved date and must be renewed. If a request is rejected, the control owner must identify and document a plan of action to reach compliance with this policy.

## 7. Policy Compliance

Adherence to this policy will be verified through various methods, including but not limited to, periodic walk-throughs, internal and external audits, metrics, and feedback to the policy owner.

## 8. Policy Violations

Any known violations of this policy should be reported to the InfoSec GRC team at grc@hq.bill.com. Any Bill.com user found to have violated any policy, standard or procedure may be subject to disciplinary action, up to and including termination of employment.

## 9. Related Policies, Standards, and Procedures

| **Policy, Standard, and Procedure** | **Purpose** |
|---|---|
| Written Information Security Program (WISP) | Provides definitive information on the prescribed measures used to establish and enforce the information security program at Bill.com. |
| Information Security Policy | Provides the directives that will ensure the highest degree of safeguarding of the data we collect, process, transmit and store. |
| Data and Information Classification Policy | To ensure that information is classified and |

| | |
|---|---|
| | protected in accordance with its importance to the organization. |
| Data and Information Handling Standard | Defines handling procedures for information in the various classification categories. |
| End User Device Standard | Establishes provisions for using, configuring, acquiring, accessing, maintaining, protecting, and securing end-user computing devices. |

## 10. References

### 10.1 Bill.com Resources

Bill.com Policies and Procedures Wiki

### 10.2 Laws, Rules, Regulations & Other Requirements

- Sarbanes Oxley (SoX)
- New York Department of Financial Services (NYDFS)
- Health Insurance Portability and Accountability Act (HIPAA)
- General Data Protection regulation (GDPR)
- California Consumer Protection Act (CCPA)
- Payment Card Industry - Data Security Standard (PCI - DSS)
- FTC Safeguards

### 10.3 Best Practices

- National Institute of Standards and Technology (NIST)
- International Standards Organization (ISO) 27001 and 27002
- Secure Controls Framework (SCF)

### 10.4 Control References

Key Control Mapping: **NIST CSF**: PR.PT-2; **SCF**: CFG-04, HRS-05, HRS-05.1, HRS-05.5, NET-12.2; **ISO 27001**: A.8.1.3

## 11. Point of Contact

For questions on this policy or to escalate potential violations, please contact the InfoSec Governance Risk and Compliance (GRC) team at grc@hq.bill.com.

## 12. Terms and Definitions

None

## Revision History

| Version | Date | Author | Revisions | Approved By |
|---|---|---|---|---|
| 2.0 | 2/19/2022 | IT Team | Annual Review | Jonathan Chan |
| 2.0 | 3/10/2022 | Infosec GRC | Annual Review | Netsai Massetti |
| 2.0 | 10/24/2022 | Infosec GRC | Update made to section 4.1 | Netsai Massetti |